PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-134181
(43)Date of publication of application : 18.05.2001

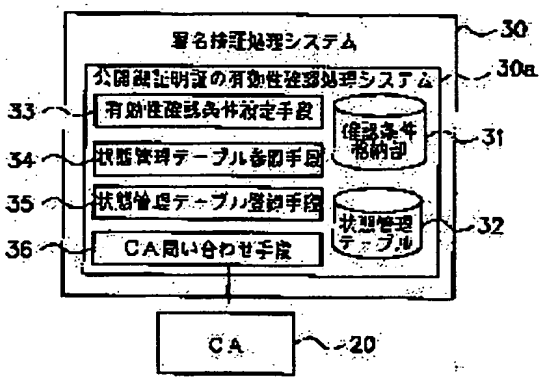
(51)Int.Cl. G09C 1/00

(21)Application number : 11-311902
(22)Date of filing : 02.11.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HASHIMOTO SHOICHI
NAKAHARA SHINICHI

(54) EFFECTVENESS CONFIRMATION SYSTEM FOR PUBLIC KEY CERTIFICATE AND METHOD THEREFOR AND MEDIUM RECORDED WITH ITS PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system capable of confirming the effectiveness of a public key certificate corresponding to the request of a signature verifying system by CA access smaller than that in the conventional system while reliablity of the system does not depend on the managing policy of a CA, and a method therefor and medium on which its program is recorded.
SOLUTION: When the effectiveness confirming and processing requests of a public key certificate is generated, whether the confirming of the effectiveness satisfying conditions in a confirmation condition storage part 31 is possible or not with respect to the certificate is confirmed from a status management table 32 by a status management table referring means 34 and when the confirming of the effectiveness of the certificate is possible, this system returns status information to the origin of the request and, besides, when it is impossible, the system requests the confirmation to a CA 20 by using a CA inquiry means 36 and the system registers the result of the confirmation and the data and hour when the status is confirmed in the management table 32 by a status management table registering means 35 and also the system returns status information to the origin of the request.



LEGAL STATUS

[Date of request for examination] 30.10.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3466975

(19)日本国特許庁(JP)　(12)特許公報（Ｂ２）　(11)特許番号

特許第３４６６９７５号
（Ｐ３４６６９７５）

(45)発行日　平成15年11月17日(2003.11.17)　(24)登録日　平成15年8月29日(2003.8.29)

(51)Int.Cl.[7]　識別記号　Ｆ Ｉ
Ｈ０４Ｌ　9/08　Ｈ０４Ｌ　9/00　６０１　Ｂ
６０１　Ｆ

請求項の数６　(全８頁)

(21)出願番号　特願平11-311902

(22)出願日　平成11年11月2日(1999.11.2)

(65)公開番号　特開2001-134181(P2001-134181A)
(43)公開日　平成13年5月18日(2001.5.18)
審査請求日　平成13年10月30日(2001.10.30)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72)発明者　橋本　正一
東京都千代田区大手町2丁目3番1号　日本電信電話株式会社内
(72)発明者　中原　慎一
東京都千代田区大手町2丁目3番1号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】公開鍵証明証の有効性確認システム及びその方法並びにそのプログラムを記録した媒体

1

(57)【特許請求の範囲】

【請求項１】　ＣＡが管理・発行する証明証であって署名検証に用いる公開鍵証明証が無効化されていないことを確認するための公開鍵証明証の有効性確認システムにおいて、

署名検証に用いる公開鍵証明証の有効性を確認した最新の日時が公開鍵証明証の有効性確認処理要求の発生時からみて何時間以内であれば良いかの条件を格納する確認条件格納部と、

公開鍵証明証の有効性を確認した時の確認結果が有効か無効かの状態情報を状態確認日時とともに格納する状態管理テーブルと、

署名検証に用いる公開鍵証明証の無効化の有無をＣＡへ確認依頼するＣＡ問い合わせ手段と、

初期設定時に、前記確認条件格納部に前記確認条件を設

2

定する有効性確認条件設定手段と、

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部に設定された確認条件を満たすか否かを状態管理テーブルの状態確認日時より確認し、確認条件を満たす場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、確認条件を満たさない場合は、ＣＡ問い合わせ手段を起動する状態管理テーブル参照手段と、

ＣＡ問い合わせ手段によりＣＡから取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブルへ登録するとともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却する状態管理テーブル登録手段とを具備することを特徴とする公開鍵証明証の有効性確認システム。

【請求項２】　公開鍵証明証の有効性確認処理要求の発

生時から予め設定した所定の時間を差し引いた日時が、状態管理テーブル内の状態確認日時以前であれば確認条件を満たすとすることを特徴とする請求項１記載の公開鍵証明証の有効性確認システム。

【請求項３】　ＣＡが管理・発行する証明証であって署名検証に用いる公開鍵証明証が無効化されていないことを確認するための公開鍵証明証の有効性確認方法において、

署名検証に用いる公開鍵証明証の有効性を確認した最新の日時が公開鍵証明証の有効性確認処理要求の発生時からみて何時間以内であれば良いかの条件を格納する確認条件格納部と、

公開鍵証明証の有効性を確認した時の確認結果が有効か無効かの状態情報を状態確認日時とともに格納する状態管理テーブルとを用い、

初期設定時に、前記確認条件格納部に前記確認条件を設定し、

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部に設定された確認条件を満たすか否かを状態管理テーブルの状態確認日時より確認し、

確認条件を満たす場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、

確認条件を満たさない場合は、署名検証に用いる公開鍵証明証の無効化の有無をＣＡへ確認依頼し、

ＣＡから取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブルへ登録するとともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却することを特徴とする公開鍵証明証の有効性確認方法。

【請求項４】　公開鍵証明証の有効性確認処理要求の発生時から予め設定した所定の時間を差し引いた日時が、状態管理テーブル内の状態確認日時以前であれば確認条件を満たすとすることを特徴とする請求項３記載の公開鍵証明証の有効性確認方法。

【請求項５】　ＣＡが管理・発行する証明証であって署名検証に用いる公開鍵証明証が無効化されていないことを確認するための公開鍵証明証の有効性確認プログラムを記録した媒体において、

前記プログラムはコンピュータに読み取られた際、該コンピュータに、

署名検証に用いる公開鍵証明証の有効性を確認した最新の日時が公開鍵証明証の有効性確認処理要求の発生時からみて何時間以内であれば良いかの条件を格納する確認条件格納部と、

公開鍵証明証の有効性を確認した時の確認結果が有効か無効かの状態情報を状態確認日時とともに格納する状態管理テーブルとを設け、

初期設定時に、前記確認条件格納部に前記確認条件を設定し、

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部に設定された確認条件を満たすか否かを状態管理テーブルの状態確認日時より確認し、

確認条件を満たす場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、

確認条件を満たさない場合は、署名検証に用いる公開鍵証明証の無効化の有無をＣＡへ確認依頼し、

ＣＡから取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブルへ登録するとともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却する処理を実行させることを特徴とする公開鍵証明証の有効性確認プログラムを記録した媒体。

【請求項６】　公開鍵証明証の有効性確認処理要求の発生時から予め設定した所定の時間を差し引いた日時が、状態管理テーブル内の状態確認日時以前であれば確認条件を満たすとすることを特徴とする請求項５記載の公開鍵証明証の有効性確認プログラムを記録した媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子署名を検証する際に用いる公開鍵証明証の有効性を確認するためのシステム及びその方法並びにそのプログラムを記録した媒体に関するものである。

【０００２】

【従来の技術】公開鍵暗号を用いた電子署名技術により、利用者の本人確認や通信路における改竄の有無の確認を行うシステムでは、認証機関（ＣｅｒｔｉｆｉｃａｔｉｏｎＡｕｔｈｏｒｉｔｙ：以下、ＣＡと略す。）が発行する公開鍵証明証を用いて電子署名の検証が行われる。公開鍵証明証には、信頼性を低下させないために利用可能な有効期間が定められているが、公開鍵に対応する秘密鍵の漏洩や所有者の身元情報の変更等の理由により、有効期間内であってもＣＡが残りの有効期間内の効力を強制的に無効化する場合がある。このため、電子署名を検証する際には、公開鍵証明証がＣＡによって無効化されていないことを確認して利用する必要がある。

【０００３】ここで、署名検証に用いる公開鍵証明証が無効化されていないことを確認する方法としては、ＣＡが定期的に発行するＣＲＬ（ＣｅｒｔｉｆｉｃａｔｅＲｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）と呼ばれる無効化された公開鍵証明証のリストをＣＡから取得して確認する方法や、ＣＡに公開鍵証明証の状態を直接問い合わせる方法等があった。

【０００４】図１（ａ）はＣＲＬを取得して確認する場合のシステム構成を示すもので、署名検証処理システム１０内のＣＲＬ取得手段１１により定期的にＣＡ２０からＣＲＬを取得し、これを記憶部１２に格納しておき、署名検証が必要となった時に公開鍵証明証有効性確認処理システム１０ａ内のＣＲＬ検索手段１３により、記憶

部１２を検索して確認する。この方法では、定期的にＣＡ２０からＣＲＬを取得しているため、署名検証時にＣＡ２０にアクセスすることなく、最も新しく取得したＣＲＬを用いて公開鍵証明証の無効化の有無を確認することになる。

【０００５】また、図１（ｂ）はＣＡに直接確認する場合のシステム構成を示すもので、署名検証が必要となった時に公開鍵証明証有効性確認処理システム１０ｂ内のＣＡ問い合わせ手段１４により、ＣＡ２０に直接問い合わせて確認する。この方法では、ＣＡ２０にアクセスした時点における公開鍵証明証の無効化の有無を確認できることになる。

【０００６】

【発明が解決しようとする課題】前者のＣＲＬを取得して確認するシステムの場合、最新のＣＲＬを取得した以降に無効化された公開鍵証明証の情報は、次のＣＲＬが発行されるまで確認することができないため、署名検証に用いる公開鍵証明証が、最新のＣＲＬを取得した以降の日時において無効化されていないことを確認することができない。従って、このＣＲＬの発行間隔が長いほど、署名検証時における公開鍵証明証の有効性確認処理の信頼性が低下するという課題があった。また、ＣＲＬの発行間隔はＣＡの運業方針によって定められることから、ＣＡの運営方針によってシステムが行う署名検証処理の信頼性が左右されてしまうという課題があった。

【０００７】一方、後者のＣＡに直接確認するシステムの場合、問い合わせた時点における公開鍵証明証の無効化の有無を確認することができるため、システムがＣＡに対して確認要求を出すことによって、署名検証時における公開鍵証明証の有効性を常に確認することができる反面、その確認の度にＣＡへのアクセスが生じ、通信コストがかかるという課題があった。

【０００８】本発明の目的は、ＣＡの運営方針に信頼性が左右されることなく、かつ従来より少ないＣＡアクセスによって、署名検証処理システムの要求に応じた公開鍵証明証の有効性を確認し得る公開鍵証明証の有効性確認システム及びその方法並びにそのプログラムを記録した媒体を提供することにある。

【０００９】

【課題を解決するための手段】図２は本発明のシステム構成を示すもので、図中、２０はＣＡ、３０は本発明の公開鍵証明証有効性確認処理システム３０ａを含む署名検証処理システムであり、公開鍵証明証有効性確認処理システム３０ａは、確認条件格納部３１、状態管理テーブル３２、有効性確認条件設定手段３３、状態管理テーブル参照手段３４、状態管理テーブル登録手段３５及びＣＡ問い合わせ手段３６を具備している。以下、これらの各手段の詳細について説明する。

【００１０】・確認条件格納部３１

システム要求として署名検証に用いる公開鍵証明証の有効性を少なくともいつの時点まで確認することが必要であるかの条件（確認条件）を格納する記憶領域。

【００１１】・状態管理テーブル３２

図３に示すように、公開鍵証明証（ここではその識別情報）に対応してこれが有効か無効かの状態情報を状態確認日時とともに格納する記憶領域。

【００１２】・有効性確認条件設定手段３３

システム初期設定時に、前記確認条件格納部３１に前記確認条件を設定する手段。

【００１３】・状態管理テーブル参照手段３４

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部３１に設定された確認条件を満たす有効性の確認が可能か否かを状態管理テーブル３２より確認し、確認可能な場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、確認不可能な場合は、ＣＡ問い合わせ手段３６を起動する手段。

【００１４】・状態管理テーブル登録手段３５

ＣＡ問い合わせ手段３６によりＣＡ２０から取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブル３２へ登録する（この際、同一の公開鍵証明証識別情報に対する状態情報が既に存在している場合には、その情報を更新する。）とともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却する手段。

【００１５】・ＣＡ問い合わせ手段３６

署名検証に用いる公開鍵証明証の無効化の有無をＣＡ２０へ確認依頼する手段（図１の（ｂ）中のＣＡ問い合わせ手段１４と同一）。

【００１６】次に、上記の各構成要素による公開鍵証明証の有効性確認方法の流れを、図４を用いて説明する。

【００１７】（１）システム初期設定時において、有効性確認条件設定手段３３により、署名検証に用いる公開鍵証明証の有効性を、少なくともいつの時点まで確認することが必要であるかの条件を、確認条件格納部３１に格納する。

【００１８】（２）署名検証処理システム３０が署名検証に用いる公開鍵証明証の有効性を確認する必要が発生した際、まず、状態管理テーブル参照手段３４により、その公開鍵証明証に対し、確認条件格納部３１に設定された条件を満たす有効性の確認が既に行われているか（確認可能か否か）を、状態管理テーブル３２より確認する。そして、その条件を満たした有効性が確認されるか、あるいは無効化されていることが確認された場合、その状態情報を状態確認処理の要求元、即ち署名検証処理システム３０に返却して状態確認処理を終了する。また、そのどちらも確認されなかった場合、つまり確認条件外の有効性が確認されるか、あるいはその公開鍵証明証の状態情報が状態管理テーブル３２内に存在しなかった場合には（３）に進む。

【００１９】（３）ＣＡ問い合わせ手段３６を用いて、署名検証に用いる公開鍵証明証の無効化の有無を、ＣＡ２０へアクセスして確認する。

【００２０】（４）状態管理テーブル登録手段３５により、（３）でＣＡ２０から取得した公開鍵証明証の有効性確認結果とその状態確認日時を状態管理テーブル３２内に登録し、その後、その状態情報を状態確認処理の要求元に返却して確認処理を終了する。

【００２１】以上説明したシステム及び処理方法を用いることにより、署名検証に用いる公開鍵証明証の有効性を確認する際、ＣＡに問い合わせた公開鍵証明証の有効性の確認結果を状態管理テーブルに保管し、その情報を以降の公開鍵証明証の有効性確認処理で活用することが可能になる。

【００２２】従って、署名検証に用いる公開鍵証明証に対して、状態管理テーブル内の情報を用いて署名検証処理システムの要求条件を満たす有効性が確認可能な場合には、ＣＡへのアクセスが不要となるため、従来よりも少ないＣＡアクセス回数により、署名検証処理システムの要求に応じた公開鍵証明証の有効性確認が可能となる。

【００２３】なお、本発明は、ＣＰＵ、メモリ、外部記憶装置等のコンピュータシステム（ハードウェア）とともに、図４の流れ図に示される手順を備えたプログラム（ソフトウェア）を記録した媒体によって実現することもできる。

【００２４】

【発明の実施の形態】次に、図５、６、７及び８を用いて、本発明の実施の形態を説明する。

【００２５】まず、システム初期設定時において、署名検証処理システムが要求する公開鍵証明証の有効性確認条件の設定について、図５を用いて説明する。

【００２６】本実施の形態では、システムが署名検証に用いる公開鍵証明証は、少なくともその署名検証時の１２時間前までの有効性が確認されていることを、公開鍵証明証の有効性確認処理におけるシステムの要求条件であると仮定する。

【００２７】・状態確認条件設定手段３３

（ａ）システム初期設定時において、システムの要求条件である公開鍵証明証の有効性確認条件を設定するため、エディタ機能を用いて、仮定した条件に対応する

「（署名検証時の日時）－（１２時間）＜（状態管理テーブル内の状態確認日時）」

の条件式を記述する。この条件式は、状態管理テーブル３２内の状態確認日時が、署名検証時の日時の１２時間前よりも後の日時を示すことを意味する。エディタ機能は、コンピュータシステムにおいて一般的に利用可能な機能である。

【００２８】（ｂ）ファイル入出力機能を用いて、（ａ）の確認条件を確認条件格納部３１に保管する。ファイル入出力機能は、コンピュータシステムにおいて一般的に利用可能な機能である。

【００２９】次に、公開鍵証明証の有効性を確認する際に、状態管理テーブル３２で有効性が確認できなかった場合に、ＣＡにアクセスしてその有効性を確認するようすを、図６を用いて説明する。図６の実施の形態では、１９９９年６月２１日１５時に、公開鍵証明証の状態確認処理が要求されたと仮定し、また、その時点における状態管理テーブルは、図７の（ａ）の状態であったと仮定する。

【００３０】・状態管理テーブル参照手段３４

（ａ）まず、公開鍵証明証解析機能を用いて、署名検証に用いる公開鍵証明証からその識別情報である発行者名、所有者名、通し番号の情報を取得する。本実施の形態では、発行者名が「ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」である識別情報が取得できたものとする。公開鍵証明証解析機能は、例えば公開鍵証明証の標準形式であるＸ．５０９形式の公開鍵証明証の内容を解析する機能が既に実現されており、容易に利用可能である。

【００３１】（ｂ）次に、ファイル入出力機能を用いて、システム初期設定時に格納した確認条件格納部３１から有効性確認条件を参照し、この確認条件式の左辺を計算するため、時刻計算機能を用いて署名検証時の日時の１２時間前を計算し、「（１９９９年６月２１日１５時）－（１２時間）＝（１９９９年６月２１日３時）」を算出する。時刻計算機能は、時刻を扱うコンピュータシステムにおいて一般的に実現されている機能である。

【００３２】（ｃ）続いて、テーブル参照機能を用いて、（ア）（ａ）で取得した公開鍵証明証の識別情報（発行者名が「ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」）で、かつ（イ）（ｂ）の計算結果と確認条件式から「１９９９年６月２１日３時＜状態管理テーブル内の状態確認日時」を満たし、かつ

（ウ）状態情報が「有効」である情報が、状態管理テーブル３２内に存在するかを確認する。

【００３３】この（ア）～（ウ）の全ての条件に合致する情報が存在した場合、署名検証に用いる公開鍵証明証の有効性が、少なくとも１２時間前以内に確認されていることになり、システムが要求する確認条件を満たすことになる。本実施の形態においては、図７の（ａ）に示されている状態管理テーブルに、（ア）～（ウ）の全ての条件に合致する情報は存在しないため、次の処理に進む。テーブル参照機能は、例えば市販のＤＢシステム等で実現されているＤＢ参照機能等が利用可能である。

【００３４】・ＣＡ問い合わせ手段３６

（ｄ）（ｃ）で、条件に合致する情報が状態管理テーブル３２内に存在しなかったため、ＣＡサービスアクセス機能を用いて、発行者名が［ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」の識別情報を持

つ公開鍵証明証の無効化の有無についてＣＡへ確認依頼する。本実施の形態では、ＣＡから状態確認結果として「有効」の情報が返却されたとする。公開鍵証明証の状態を確認するためのＣＡサービスアクセス機能は、例えば既存のＣＡが提供する公開鍵証明証検証サービス等を利用することにより実現可能である。

【００３５】・状態管理テーブル登録手段３５

（ｅ）（ｄ）で確認依頼を行った日時情報とＣＡから返却された対象公開鍵証明証の有効性確認結果を、テーブル更新機能を用いて、状態管理テーブル３２内の発行者名が「ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」の識別情報に対応する状態確認日時情報と状態情報の欄に上書きする。本実施の形態では、ＣＡへの状態確認日時が、１９９９年６月２１日１５時００分１０秒に完了したと仮定している。図７の（ｂ）に更新後の状態管理テーブル３２の状況を示しておく。テーブル更新機能は、例えば市販のＤＢシステムにおいてＤＢの情報を書き換えるためのＤＢ更新機能等が利用可能である。

【００３６】（ｆ）その後、戻り値返却機能を用いて公開鍵証明証の状態確認処理の要求元に状態情報を返却して確認処理を終了する。戻り値返却機能は、通常のプログラム作成において利用可能な機能である。

【００３７】続いて、公開鍵証明証の有効性をＣＡにアクセスせずに、状態管理テーブルの参照のみで確認可能となる実施の形態について、図８を用いて説明する。図８は、図６の処理の後、再度同一の公開鍵証明証を用いた署名検証処理が行われた場合の実施の形態を示しており、１９９９年６月２１日１６時に公開鍵証明証の状態確認処理が開始され、また、この時点における公開鍵証明証の状態管理テーブルは、図７の（ｂ）に示す状態であったとして説明する。

【００３８】・状態管理テーブル参照手段３４

（ａ）公開鍵証明証の状態確認処理の開始（要求）を受けて、図６の時と同様に、公開鍵証明証解析機能を用いて署名検証に用いる公開鍵証明証から識別情報の取得を行い、発行者名が「ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」である識別情報を取得する。

【００３９】（ｂ）次に、ファイル入出力機能を用いて、システム初期設定時に格納した確認条件格納部３１から有効性確認条件を参照し、この確認条件式の左辺を計算するため、時刻計算機能を用いて、署名検証時の日時の１２時間前を計算し、「（１９９９年６月２１日１６時）－（１２時間）＝（１９９９年６月２１日４時）」を算出する。

【００４０】（ｃ）続いて、テーブル参照機能を用いて、（ア）（ａ）で取得した公開鍵証明証の識別情報（発行者名が「ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」）で、かつ（イ）（ｂ）の計算

結果と確認条件式から「１９９９年６月２１日４時＜状態管理テーブル内の状態確認日時」を満たし、かつ、

（ウ）状態情報が「有効」である情報が、状態管理テーブル内に存在するかを確認する。図７の（ｂ）より、ハッチング部分の情報が上記（ア）～（ウ）の全ての条件に合致する情報であるため、戻り値返却機能を用いて公開鍵証明証の状態確認処理の要求元に状態情報である「有効」を返却して確認処理を終了する。

【００４１】上記のように、署名検証処理システムが署名検証に用いる公開鍵証明証の有効性を確認する際、その公開鍵証明証が、予め定めた署名検証に用いるための有効性確認条件に合致するかの確認を、状態管理テーブル内に登録されている、過去にＣＡに問い合わせた有効性確認結果から判断可能な場合には、ＣＡへのアクセスが不要となるため、従来よりも少ないＣＡアクセス回数により、システムの要求に応じた公開鍵証明証の有効性確認が可能となる。

【００４２】

【発明の効果】以上説明したように、本発明によれば、署名検証に用いる公開鍵証明証の有効性の確認において、過去にＣＡに問い合わせた有効性確認結果を、以降の有効性確認処理に活用することが可能となり、活用できた場合にはＣＡへのアクセスが不要となるため、短期間で同一利用者の電子署名を複数回検証する必要があるシステム等では、ＣＡアクセスのために費やされていた通信コストが削減され、署名検証処理の処理性能を向上させることが可能となる。また、１時間前、あるいは１日前等というように、署名検証時から遡っていつの時点までにおける公開鍵証明証の有効性が確認されれば良いかという条件をシステム自身が任意に設定することが可能であるため、システムの要求に応じて公開鍵証明証の有効性確認処理の正確さを制御することが可能となる。

【図面の簡単な説明】

【図１】従来の公開鍵証明証の有効性確認システムの構成図

【図２】本発明の公開鍵証明証の有効性確認システムの構成図

【図３】公開鍵証明証の状態情報を保管する状態管理テーブルの構成図

【図４】本発明の公開鍵証明証の有効性確認方法の処理の流れをシステムの構成要素とともに示す図

【図５】システムの要求に基づく有効性確認条件の設定の実施の形態を示す図

【図６】状態管理テーブルでは公開鍵証明証の有効性が確認できず、ＣＡにアクセスして確認する実施の形態の説明図

【図７】実施の形態における状態管理テーブルの内容の一例を示す図

【図８】ＣＡにアクセスせず、状態管理テーブルの参照のみで公開鍵証明証の有効性を確認可能な実施の形態の

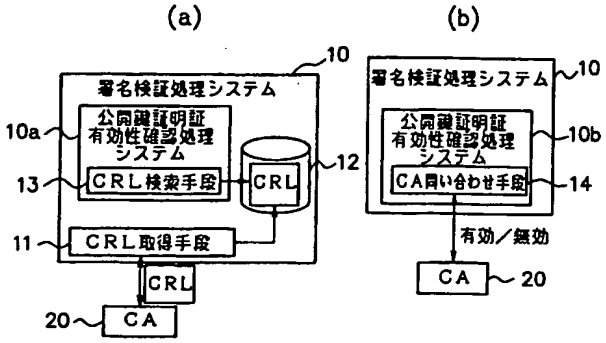
説明図

【符号の説明】

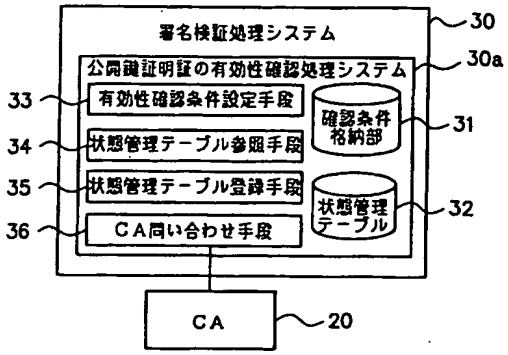
２０：ＣＡ、３０：署名検証処理システム、３０ａ：公開鍵証明証有効性確認処理システム、３１：確認条件格

納部、３２：状態管理テーブル、３３：有効性確認条件設定手段、３４：状態管理テーブル参照手段、３５：状態管理テーブル登録手段、３６：ＣＡ問い合わせ手段。

【図１】



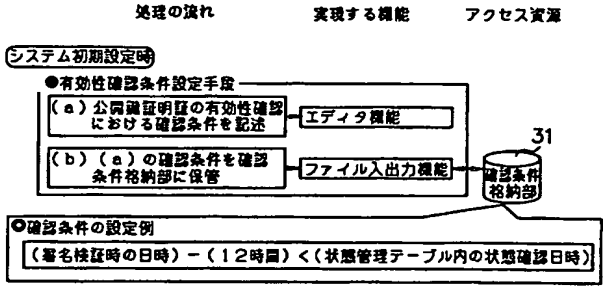
【図２】



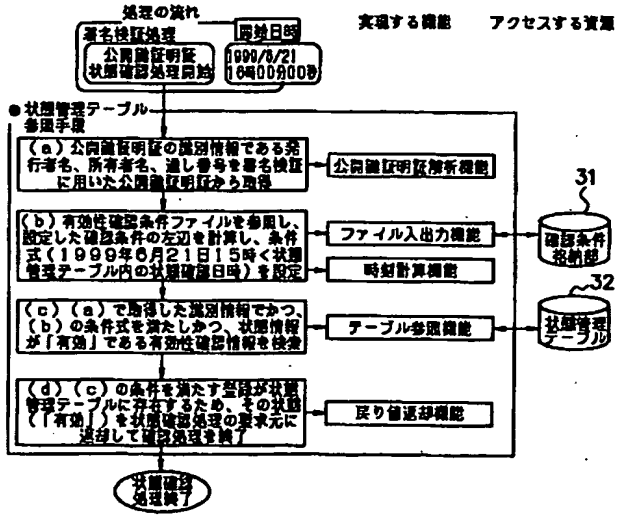
【図３】

公開鍵証明証識別情報	状態確認日時	状態
公開鍵証明証１	1999/06/20 10時20分00秒	有効
公開鍵証明証２	1999/06/20 13時00分00秒	有効
公開鍵証明証３	1999/06/21 10時00分00秒	無効

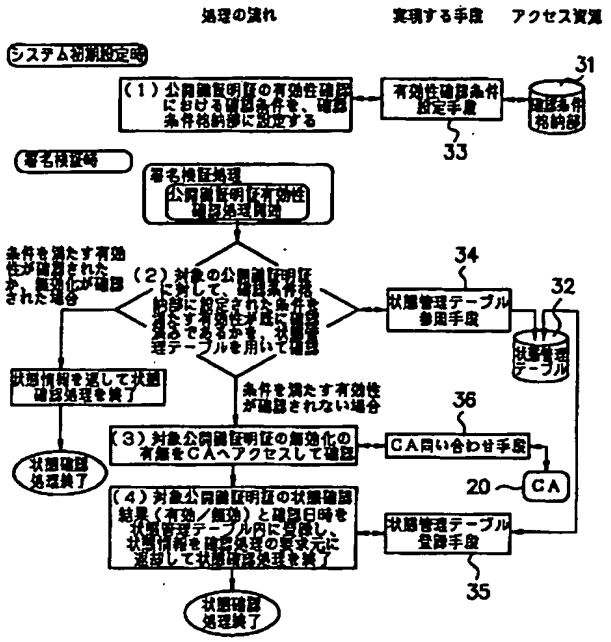
【図５】



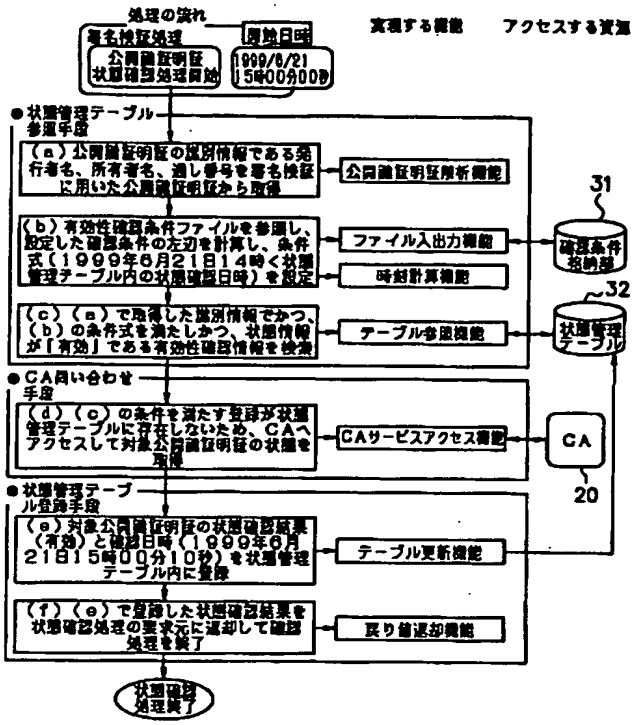
【図８】



【図４】



【図６】



【図７】

(a) 公開鍵証明書の有効性確認処理前の状態

公開鍵証明識別情報			状態確認日時	状態
発行者名	所有者名	シリアル番号		
CA－１	利用者Ａ	１００１	１９９９/０６/２０ １０時００分００秒	有効
CA－１	利用者Ｂ	１００５	１９９９/０６/２０ １３時００分００秒	有効
CA－２	利用者Ｃ	２００１	１９９９/０６/２１ １０時００分００秒	有効

(b) 公開鍵証明書の有効性確認処理後の状態

公開鍵証明識別情報			状態確認日時	状態
発行者名	所有者名	シリアル番号		
CA－１	利用者Ａ	１００１	１９９９/０６/２１ １５時００分１０秒	有効
CA－１	利用者Ｂ	１００５	１９９９/０６/２０ １３時００分００秒	有効
CA－２	利用者Ｃ	２００１	１９９９/０６/２１ １０時００分００秒	有効

フロントページの続き

(56)参考文献　Ｃａｎ　Ｗｅ　Ｅｌｉｍｉｎａｔｅ　Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｏｎ　Ｌｉｓｔｓ?，Ｌｅｃｔｕｒｅ　Ｎｏｔｅｓ　ｉｎ　Ｃｏｍｐｕｔｅｒ　Ｓｃｉｅｎｃｅ，Ｖｏｌ．1465，ｐ．178－183
公証システムにおける個人認証方式の一考察，1998年電子情報通信学会総合大会講演論文集，1998年　３月26日，基礎・境界，ｐ．256

(58)調査した分野(Int.Cl.⁷，ＤＢ名)
H04L　9/08
ＪＩＣＳＴファイル（ＪＯＩＳ）